

enable the recharger **104** when authorized use has been established (e.g., the correct security-code is entered). Actually, It will be apparent to those skilled in the art that the guardian **108** can be configured based on one or more criteria (e.g., numerous events, conditions, or situations) that indicate potential unauthorized use of the device **100**. Furthermore, various criteria can be combined with numerous actions (e.g., disable first if taken out of a geographical boundary, ask for authorization first if the timer expires, disable first if connected to an unknown device).

[0028] FIG. 1B depicts a device-protection method **150** for protecting a device against unauthorized use in accordance with one embodiment of the invention. In order to protect the device against unauthorized use, it is determined (**152**) whether to disable a recharger (e.g., a recharge-circuit) that normally charges a rechargeable-power-supply (e.g., battery) when connected to a power source (outlet). The device is powered by the rechargeable-power-supply. Accordingly, if it is determined (**152**) not to disable the recharger, the device-protection method **150** ends. However, if it is determined (**152**) to disable the recharger, the recharger is disabled (**154**). Disabling the recharger would significantly hinder normal use and enjoyment of the device, if the rechargeable-power-supply is the main source of power.

[0029] FIG. 2 depicts a device protection method **200** for protecting a device in accordance with one embodiment of the invention. The device protection method **200** can, for example, be used by the guardian **108** shown in FIG. 1A. Initially, it is determined (**202**) whether potential unauthorized use of the device can be suspected based on one or more criteria (e.g., an event, condition, or situation) that indicate potential unauthorized use of the device. As noted above, an event, condition, or situation can, for example, be the expiration of a timer, connection or communication with another object (e.g., another device, adaptor, server), or locating the device outside of defined geographical region. Accordingly, if unauthorized use is suspected (**202**), the recharger is disabled (**204**) so that the recharger cannot charge the rechargeable-power-supply. Subsequently, it is determined (**208**) whether use of the device can be authorized. The use of device can, for example, be authorized by requiring a security-code to be entered, requiring that the device be connected to a known device, or moving the device back to a geographical boundary. If it is determined (**210**) that the use of the device is authorized, the recharger is enabled (**212**) so that it can recharge the rechargeable-power-supply. Thereafter, the device-protection method **200** proceeds to determine (**202**) whether unauthorized use of the device is suspected and proceeds in a similar manner as discussed above. However, if it is determined (**208**) that the use of the device cannot be authorized, it is determined (**210**) whether to allow reauthorization (e.g., allow reentering of a security-code). If it is determined (**210**) to allow reauthorization, the authorized use of the device is determined (**208**). As a result of the reauthorization, the recharger may be enabled (**212**). However, if no reauthorization is allowed (**210**), the device-protection method **200** ends and the recharger is left disabled rendering the device inoperable when the recharger that powers the device eventually runs out.

[0030] FIG. 3A depicts a device **300** which is protected by a guardian **302** from unauthorized use in accordance with

another embodiment of the invention. The guardian **302** detects connection to an unauthorized object (e.g., adaptor, PC, server). More particularly, if the device **300** is directly or indirectly connected to a power source **312** and/or connects or communicates with another device, the guardian **302** effectively determines whether such activity is unauthorized. In other words, guardian **302** determines whether the adaptor **304** and/or device **308** are authorized for use with the device **300**. Those skilled in the art will appreciate that this determination can, for example, be made based on a unique identification (ID) assigned to an adaptor, computer, or other components. Typically, various components used in computing systems have a unique assigned ID (e.g., processor ID, Adaptor ID). Hence, the guardian **302** can, for example, determine the ID for the adaptor and/or other device **308** as soon as connection is made to the device **300**. Subsequently, the guardian **302** can determine whether the ID has been authorized by determining whether the ID is among a number of IDs that have been authorized for the device **300**. As shown in FIG. 3A, a number of IDs that have been authorized for the device can, for example, be stored in memory **310** on the device and/or stored in a central authorization location **314** and provided to the device upon request. If an ID is not authorized, the guardian **302** can initiate an authorization process. The authorization process can, for example, request a security-code to be entered by the user. In one embodiment, the security-code can be defined by the user of a media-player as an item associated with the media-player (e.g., a song, a movie, a folder). It should be noted that the device **300** can also include a Global Positioning System (GPS) **320** and a timer **321**.

[0031] FIG. 3B depicts a device protection method **350** for protecting a device in accordance with one embodiment of the invention. Initially, it is determined (**352**) whether the device has been connected to a component (e.g., another device, a server, an adaptor). If it is determined (**352**) that the device has been connected to a component, an identifier (e.g., device ID, adaptor ID, processor ID) for the device is determined (**354**). Typically, this identifier is a unique identifier that has been assigned to the device. Accordingly, it is determined (**356**) whether the identifier is authorized. If it is determined (**356**) that the identifier is authorized, it is determined (**352**) whether the device has been connected to a component. In other words, the connection to a first component is effectively ignored when the connection is determined to be authorized, and it is determined whether another component has been connected to the device.

[0032] However, if it is determined (**356**) that the identifier is not authorized, it is requested (**358**) that a security-code be entered to authorize the component. Next, it is determined (**360**) whether the security-code is received. If it is determined (**360**) that the security-code has been received, it is determined (**362**) whether the security code is correct. If it is determined (**362**) that the security-code is correct, it is determined whether the device is connected to a component (i.e., another component). In other words, the connection of the device to the first component is effectively ignored if it is determined (**362**) that the correct security-code has been received. On the other hand, if it is determined (**362**) that the security-code is not correct, one or more opportunities may be given (**364**) to enter the correct security-code. However, if the correct security-code is not received, for example, after a determined number of tries or passage of a predetermined amount of time, the recharger that is used to